

Ser. No. 10/030,766
Internal Docket No. RCA 89,520
July 24, 2006

RECEIVED
CENTRAL FAX CENTER
JUL 24 2006

Remarks/Arguments

Claims 1-7 and 9-10 are pending.

Rejection of claims 1-7 and 9 under 35 USC 103(a) as being unpatentable over Kaganas et al. (US 6425018) and Truong et al. (US Pat No 6173057)

Applicants submit that for at least the reasons discussed below the present amended claims are patentably distinguishable over the cited combination of Kaganas and Truong.

Amended claim 1 recites "... determining a unique identification associated with the removable data storage device coupled to the handheld audio playback device, and **decrypting the audio data file using the unique identification and decrypting the associated decoder file using a first key**; decoding the decrypted audio data file in accordance with the decrypted decoder file in the digital signal processor..." Applicants submit that neither Kaganas nor Truong disclose or suggest this limitation of amended claim 1.

The office action acknowledges that Kaganas fails to teach the step of decrypting the audio data file using a unique identification associated with the storage device. Truong is cited to provide the missing element.

Applicants respectfully submit that Truong fails to provide the missing element. Truong teaches a system that uses a **separate** recording medium having information stored thereon, and a portable medium (e.g. smart card) having security information stored thereon for enabling a user to access the information on the recording medium using a computer platform (col. 4, lines 5-14). The recording medium is a non-rewritable medium, wherein the contents of the medium can be read but not modified or altered (col. 3, lines 8-10).

The recording medium may include an identity parameter specific to the medium to secure the recording medium (col. 3, lines 22-24). However, the identity parameter associated with the recording medium is not associated at all with a step of decrypting data files stored on the recording medium. Rather, the identity parameter is used by the hardware security device to **confirm the identity of the recording medium** during the first step of the process for accessing data

Ser. No. 10/030,766
Internal Docket No. RCA 89,520
July 24, 2006

on the medium (col. 4, lines 24-37). Once the identity of the recording medium has been confirmed, various steps are performed to authenticate the integrity of the software on the recording medium using various signatures stored on the recording medium (col. 4, lines 38-44). Then, various security checks are performed to ensure proper security levels and that there have been no breaches of the method (col. 4, line 59 - col. 5, line 22). Nowhere does Truong teach or suggest that the identity parameter of the recording medium is used to decrypt the data files stored on the recording medium.

The portions of Truong cited by the Office Action fail to teach or suggest the above cited limitation of claim 1. Col. 3, lines 10-16 mention that in the first stage of the process the information to be protected, the operating systems for the information, and a set of security and control parameters are defined. Col. 3, lines 22-26 mention that the security parameters may include an identity parameter specific to the medium, and lines 34-41 mention that some or all of the information may be encoded or encrypted. Finally, col. 4, lines 5-10 mention that the publisher supplies the recording medium and a portable medium (e.g. a smart card), wherein the smart card may include identity code **specific to the user** and keys for decoding or decrypting information stored on the recording medium. However, nowhere does Truong mention or suggest decrypting the data files on the recording medium using the identity parameter of the recording medium. Rather, Truong specifically mentions that the identity parameter is used in the first step to **verify the identity of the recording medium**.

By contrast, the present invention contemplates that the removable data storage device may be a rewritable recording medium wherein the data may be copied from another memory device using file management software (page 9, lines 13-15). In that regard, the present invention uses the unique identification in the manner recited to prevent an audio player from playing an audio data file that was copied from another memory card, thereby providing a layer of protection (page 9, lines 15-17). Truong does not teach or suggest such a limitation because Truong specifies using a non-rewritable medium.

In view of the above, applicant submit that even if Kaganas is combined with Truong in the manner suggested, the proposed combination still fails to teach or suggest each and every limitation of present claim 1. Thus, applicants submit